VOLUME 42, AUTUMN 1999

DATAWATCH

is a quarterly magazine
published by the

Information Systems Audit and Control Association
London Chapter

Editorial Team:
Annabel Lane
Andy Farrington
John Hunter
Nancy Watt

To advertise:
Call Nancy Watt on:
01487 815705
or Email:
Isacalondn@aol.com
Website:
http://members.aol.com/isacalondn
Chapter Office:
10 Drayhorse Road
Ramsey, Huntingdon
Cambs PE17 1SD

DATAWATCH is published by the Information Systems Audit and Control Association London Chapter, membership of the chapter entitles one to receive an annual subscription to DATAWATCH.

Opinions expressed in DATAWATCH represent the views of the authors. They may differ from policies and official statements of the ISACA London Chapter and its committee, and from opinions endorsed by authors' employers, or the editorial team of this magazine. ISACA London Chapter does not attest to the originality of the authors'content.

FEATURES

In this issue:

REGULARS

PLUS

ISACA London Chapter Committee 1999/2000

PRESIDENT
John Mitchell
LHS Business Consultancy
01707 851454
Lhs001@aol.com

VICE PRESIDENT
Steve Bailey
Steve Bailey Associates
01480 432602
Spart@compuserve.com

TREASURER
Archie Watt
BDO Stoy Hayward
0171 893 2671
Archie.Watt@bdo.co.uk

SECRETARY
Charles Mansour
The Woolwich
0181 298 5646
Charles.Mansour@woolwich.co.uk

MEMBERSHIP
Kamal Khan
Sanwa Bank Ltd
0171 330 5522
kamal.khan@sanwabank.co.uk

PUBLICATIONS
Annabel Lane
Nestle UK Ltd
0181 667 6530
annabel.lane@nestlegb.nestle.com

SIGS
John Hunter
HLB International
01635 248944
mailbox@jhunter.u-net.com

SIGS/LIBRARY
Bill Hawkins
Corporation of London
0207 332 1296
Bill.Hawkins@corpoflondon.gov.uk

MARKETING
Derek Oliver
Ravenswood Consultants
01268 794556
consultants@ravenswood:co.uk

EVENTS
Karen Sharpe
Deloitte & Touche
karen.sharpe@deloitte.co.uk

CISA CO-ORDINATOR
David Spaven
KPMG
0171 311 5620
David.Spaven@kpmg.co.uk

PAST PRESIDENT
Gerry Penfold
KPMG
0171 311 8489
Gerry.Penfold@kpmg.co.uk

CHAPTER OFFICE
Nancy Watt
10 Drayhorse Road, Ramsey, Huntingdon,
Cambs, PE17 1SD
Tel/Fax: 01487 815705
Isacalondn@aol.com
http://members.aol.com/isacalondn/

ISACA Northern UK Committee (officers only)

PRESIDENT
Ray Butler
HM Customs & Excise
0161 827 0875
rbutler.c&e.cau@gtnet.gov.uk

VICE PRESIDENT
Robert Newbould
British Steel
01709 825479
bob_newbould@technology.britishsteel.co.uk

TREASURER
Gillian Peschke
Pricewaterhouse Coopers
0113 289 4273
gillian.peschke@uk.pwcglobal.com

MEMBERSHIP
Lynn Lawton
KPMG
0161 838 4000
Lynn.Lawton@kpmg.co.uk

CISA CO-ORDINATOR
Alan Rainford
Axa Insurance
01253 662782
alan_rainford@gre-group.e-mail.com

WEB MASTER
Peter McCready
MBNA International Bank
01244 672000
macriada@btinternet.com

ACADEMIC RELATIONS
Mike O'Hara
University of Salford
0161 295 5665
m.j.ohara@iti.salford.ac.uk

WEBSITE:

ISACA.CO.UK/NORTHERN

ISACA Central UK Committee (officers only)

PRESIDENT
James Whittaker
British Telecom
0121 230 5816

PAST PRESIDENT
Lawrence Devlin
KPMG
0121 232 3201

SECRETARY
Mike Hughes
KPMG
0121 232 3207

CISA
Simon Parker
Nottingham Building Soc.
0115 956 4305

EVENTS
Geoff Adey
KPMG
0121 232 3202

WEBSITE:

ISACA.CO.UK/CENTRAL

The Editor's Chair

Well here I am, first issue with the Editor's chair all to myself and it's quite comfortable so far anyway, despite being known as "the hot seat".

However, I can't take all the credit for the impressive looking magazine that you hold in your hands as Datawatch is now being supported by a dedicated Committee and I mean that in both senses of the word. I have the role of Editor, taking the praise and/or blame; management of our bank of articles and copy is being carried out by John Hunter; Bill Hawkins is developing our commercial side and our relations with advertisers; Nancy Watt our Chapter Administrator still does the hard work in transforming the articles into the magazine itself and ensuring it gets published and Andy Farrington, the previous Editor is still on the committee, helping us ensure continuity and maintaining the ISACA London web site at present. Well, we couldn't let him get away that easily!

The more perceptive among you will have noticed that the London Chapter's events this season are revolving around a theme. This is the extended enterprise and through this we aim to explore some of the many issues facing companies today regarding ecommerce, and links to customers and suppliers, for example EDI invoicing, vendor managed inventory, and internet presence. Security and audit have an important role to play in this area and so we have tried to pick up that theme within this edition of Datawatch, with articles on e business and security as well as a congratulation to those who have been successful in the CISA exams this year.

I can't possibly conclude without mentioning that Datawatch has just scooped the award for the best Chapter newsletter for the fifth year running thanks to much hard work from all involved over the past year. The President gives more details in his column on the excitement of receiving it on our behalf. He hasn't told me yet whether he cried or who he thanked in his acceptance speech…..

NEWSBRIEF

CERTIFICATION: The new Certification Board met at Rolling Meadows from Friday 27 to Sunday 29 August chaired by Marios Damionades (E&Y, Dallas). Robert Coles from the UK Northern Chapter (KPMG, Leeds) has recently joined the Board. A mission statement and strategy for the future of ISACA certifications has been drawn up and the 2000 examination has been set. The 'pool' of questions is quite low in some domains. If anyone feels they would be able to help with writing CISA questions (Items) "to order" please let Derek Oliver know (you will get US$50 for each question accepted).

PUBLICITY: It has been agreed that the display stand needs updating - any ideas would be appreciated

RESEARCH: The Digital Signatures monograph which London Chapter instigated and supported financially has been published, see page 5 for details.

PUBLICATIONS: Two new documents are available for download from the ISACA web site: Conducting Year 2000 Reviews During the Final Months Before the Millennium and COBIT Audit Guideline for Y2K Contingency Planning. Both are ISACF publications.

Y2K LISTSERV: Archived postings from this listserv are now available at: http://y2k-contingency.sparklist.com. The purpose of the listserv is to enable IS professionals to provide information, ask questions and share knowledge on Y2K contingency planning. To join the listserv, e-mail y2k-contingency-request@share.isaca.org. In the body, type: SUBSCRIBE. This listserv is sponsored by ISACA.

From the President

By John Mitchell

I recently attended the Global Leadership Conference in Denver, Colorado where the various Chapter representatives get together to map out the way that we would like ISACA to go in the future. It was a pretty intensive, but enjoyable weekend, with me as the rookie president learning all that I could from others with more experience. The most enjoyable part was picking up a couple of awards on your behalf: the Pinnacle award for our support of the digital signatures project and a Best Newsletter Award for Datawatch. This is the fifth time that Datawatch has scooped this particular award and I used the opportunity to hand out some copies of the magazine to the other Chapter presidents. The feedback was very positive ranging from 'this is better than the one from International', through to 'I would like to subscribe to this, how can I sign up?'. What did I learn apart from us having the best magazine? Well, our range of activities easily exceeds those of most other Chapters, but then we are the second largest Chapter in the world, only being beaten by New York. The other interesting thing was that our membership subscription is relatively modest when compared to other European Chapters.

This was of particular interest to me because at our committee away day we had discussed long and hard what we should do in this area. A whole host of things were tied together: what would International do regarding their component (remember about two thirds of your subscription goes straight to them), what would the exchange rate look like in six months time, what reserve policy was prudent, what events did we want to run, what income could we generate and what would happen to printing and postage costs some 12 months down the line? This is a fairly complex equation with too many unknowns for comfort, but we did our best and concluded that a modest rise of £2 for next year was reasonable. In practice this means that we will retain about £37 of what will be a £100 subscription next year. This is below inflation and is less than most other professional bodies, but I accept that any increase is bad news unless you receive an increased level of service to compensate for the rise. Well, Datawatch is now even better than it was, we are enhancing the refreshments at the monthly meetings and re-introducing the events card, so that you can see at a glance our annual programme. I know that you will not be disappointed.

One hundred and five members passed the CISA examination this year (see the list elsewhere in this edition) and are currently applying for the right to use the designatory letters. My congratulations to them and my commiserations to those of you who did not make it this time. Keep trying. With several hundred CISA holders in the South East it is becoming almost de rigueur to have the qualification for the more senior computer audit positions.

And now to something completely different. For the last few weeks I have been helping the search for extra terrestrial intelligence (SETI). The SETI project is using spare computer time around the world to analyse radio signals from outer space for signs of life. So far about 50,000 people have signed up to the project which works on the basis of using your computer's idle moments (and most machines are only used for about two hours per day) to process a block of data which is passed to you from a central computer. Once the block is analysed it is passed back to the centre and your machine receives another one. Your involvement is minimal as the analyser is a screen saver (very pretty too) which kicks in when the machine has nothing else to do. The central computer knows who has analysed each block, so if it is your block which contains the equivalent of 'here we are', then you get the recognition. I know that Annabel has not provided this important web address in her list of interesting sites, so if you want to give it a go point your browser to www.setiathome.ssl.berkeley.edu. You never know, there may be computer auditors out there looking for signs of intelligent life over here, but please do not use your firm's machine for this.

Happy searching.

John Mitchell

NEW! ***Digital Signatures Security & Controls Monograph***

This new research deliverable addresses the technical, audit and control, legal and standards issues related to digital signature technology and will be of interest to anyone involved in business and finance today. It includes a suggested audit work program utilizing the COBIT® framework. Authored by recognized cryptography and IS control authorities, the project was sponsored by ISACF™, the London Chapter of ISACA™ and S.W.I.F.T. Digital Signatures Security and Controls can be ordered through the ISACA bookstore at bookstore@isaca.org (US $35 for members, US $50 for non-members).

EXPERTS SOUGHT!

The Research Board have requested that London Chapter seek out their members for "subject matter experts" in technical areas. The work may involve conference calls, reading and producing papers in your specialist subject.

If you feel you have something to offer, then please get in touch with Nancy, Isacalondn@aol.com.

Collection of this data will enable the board to more uniformly involve chapters and individuals in research projects.

London Chapter Events 1999-2000

The Extended Enterprise

"No man is an island" and neither is a modern enterprise. All kinds of businesses and public sector organisations have embraced networks and distributed computing within the boundaries of their organisations. With the explosion of the internet, business to business e-commerce is becoming easier and cheaper. Links to customers, suppliers and other third parties such as banks or information providers are increasing. Business processes are reaching out into other organisations, not only for transaction processing (e.g. ordering, invoicing, distribution, payments) but also for business planning (e.g. suppliers accessing customers' systems for demand planning or customers accessing suppliers systems for product information).

Technology is also enabling other efficiencies in areas such as procurement, through the use of smart cards for example, for high volume, low value purchases.

The era of e-commerce and the latest technological developments makes the concept of the Enterprise a reality today. This is a growing challenge for IS Audit and Security professionals, especially as the high performance companies of tomorrow will be exploiting the concept rapidly, challenging our current thinking on IT governance, risk management and control. What sort of enterprise will we be auditing in the next few years? The London Chapter's 1999/2000 programme of events aims to explore this theme and propose some of the answers - so come along and help shape the future!

16 September 1999
The High Performance Co
Gerry Penfold

21 October 1999
BS7799/C:Cure
Derek Oliver

18 November 1999
Development Issues in the Extended Enterprise
TBA

16 December 1999
Christmas Meeting
Annabel Lane & Andy Farrington

20 January 2000
Internet Security
TBA

17 February 2000
PKI
Zergo Baltimore

16 March 2000
Digital Signatures
Fred Piper & John Mitchell

20 April 2000
Intrusion Detection
ISS

18 May 2000
AGM &
Penetration Testing
Steve Bailey

15 June 2000
Contingency Planning for the Extended Enterprise
TBA

All meetings will take place at the offices of KPMG, 8 Salisbury Square, London EC4 commencing at 4.30pm. Meetings are free to members, a charge of £20 will be made to non-members.

Introduction to e-Business Part II

By Judy Altrudo

The previous article provided an overview of some of the business and legal issues that underpin e-commerce developments. This article looks at some of the key technology issues that are required to be either in place or developed for the successful deployment of an EC strategy.

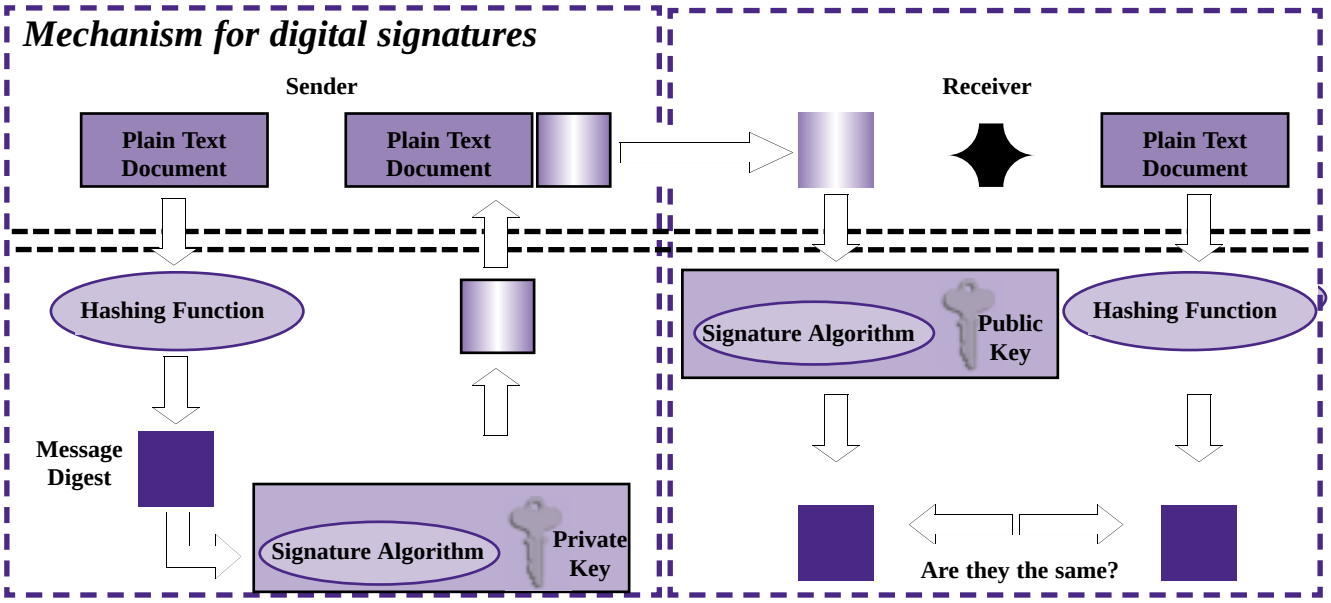
Technology Infrastructure

Successful EC companies keep abreast of changing technologies to ensure that they are knowledgeable enough to know when and how it can be exploited to meet their business objectives, and to know when it is better to create standards rather than to follow them. The main technologies break down into a number of areas, some of which can be directly affected by an EC business, others require planning and cooperation with other partners and the consumers themselves:

✦ **Network bandwidth** - Networks are traditionally considered bottlenecks but, the popular World Wide Wait acronym notwithstanding, Wide Area Network (WAN) technologies are slowly starting to address issues of speed with such developments as Asynchronous Transfer Mode (ATM) for high speed business to business links and Asymmetric Digital Subscriber Line (ADSL) providing consumers with more realistic bandwidth for downloading media-rich Internet content. This is enabling businesses to serve both more customers and more data, a typical entrepreneurial example of this being the pop-singer David Bowie who is making his latest music available for download via the Internet before releasing it on CD.

✦ **Dynamic Content** - Gone are the days of the static web page. Successful EC businesses are making use of new technologies such as Java, CORBA and ActiveX to not only provide consumers and other businesses with an enriched interaction with their systems, but are providing dynamic content by harnessing the power of On-Line Analytical Processing (OLAP) to drive data warehousing and data mining operations. This is further supported by the development of eXtensible Markup Language (XML), which harnesses some of the potential of Electronic Data Exchange (EDI) in a simple lightweight language and makes this available to both consumers and businesses. Microsoft is heavily promoting this technology with their BizTalk infrastructure.

✦ **Protocol Infrastructure** - For public computer networks like the Internet, but increasingly for



intranets, the Internet Protocol Family, popularly known as TCP/IP v4, is the de facto protocol suite. The success of the Internet is for a large part due to the widespread adoption of this protocol family. The core protocols in this family are reaching their 20th birthday, ancient in this fast-paced industry, and suffer from weaknesses in the area of addressing and security (although the forthcoming TCP/IP v6 solves some of these issues)

✦ **Security Infrastructure** - Apart from the Internet itself perhaps the most significant technology essential to a successful electronic trading environment is security. There is a major development drive in this area, and the remaining part of this paper will look more closely at the issues that need to be overcome for a successful EC deployment.

Security Requirements

Protecting sensitive information is essential to creating a secure electronic business environment. Security for business includes the protection of transactional information, corporate secrets and proprietary information and these challenges still apply in an electronic environment. But there are some new challenges as well. Security features found in the physical environment (e.g. properties of ink, characteristics of the printing process, watermarks and signature biometrics) may not be found in the electronic world. Also, some risks are peculiar to the electronic environment such as those associated with network resources.

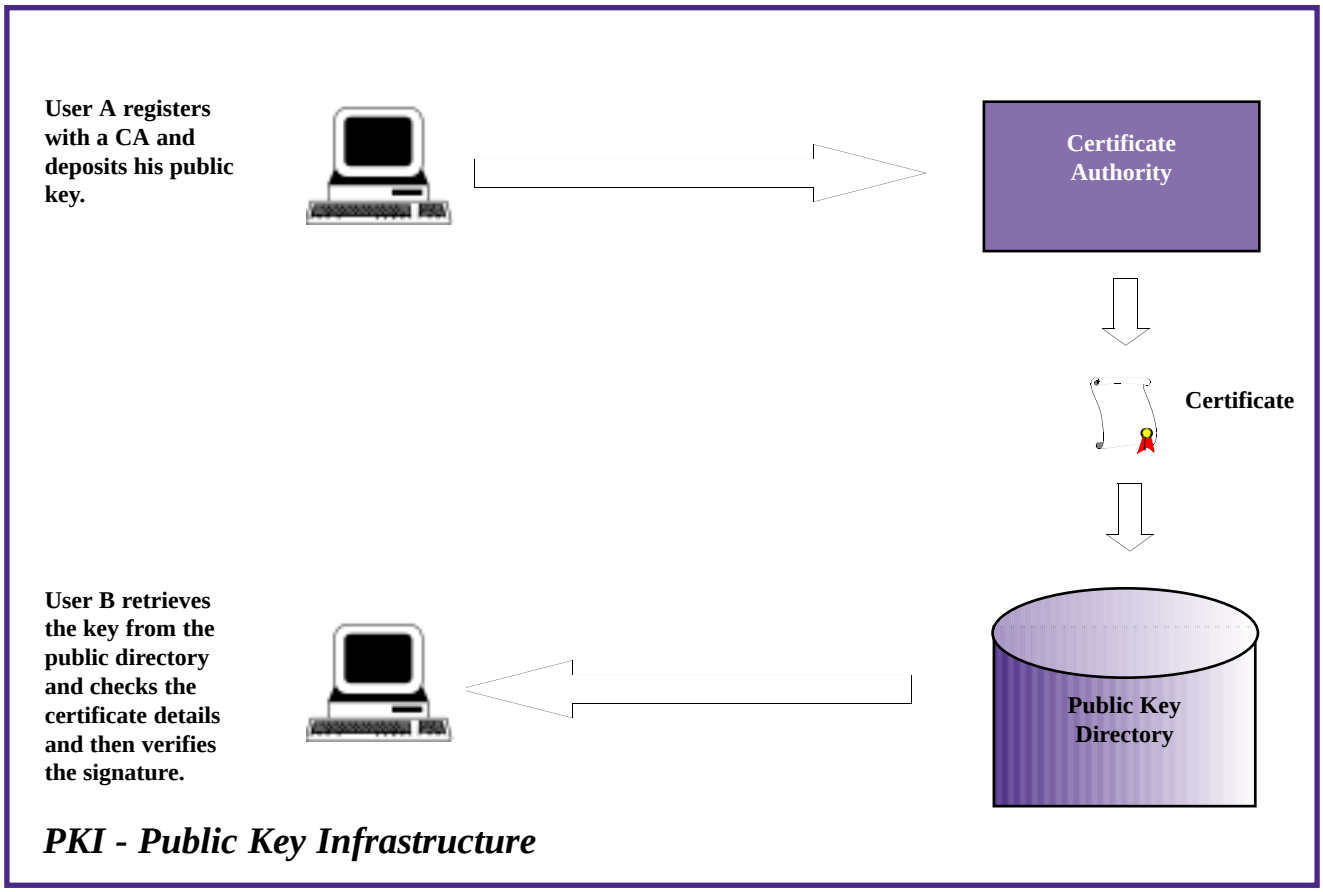
Applications and technologies for electronic commerce must address security issues and incorporate controls for: authentication (to ensure that we can positively identify who we are trading with); authorisation (to ensure that our assets are protected and are only accessible to those who have a right); confidentiality (to ensure that sensitive information is protected during transmission and when stationary); integrity (to ensure that the our information assets may be relied upon); and non-repudiation (to ensure that transactions in the market place cannot just simply be denied).

Cryptography

Cryptography is a collection of techniques for keeping information (or plain text) secure by transforming it into something that is unintelligible (cipher text) to an unauthorised recipient. An authorised recipient requires a key that will enable the encrypted message (cipher text) to be transformed back to its original form.

Cryptography that is used to provide **authentication services** is achieved through the use of digital signatures. This technique may also be used to provide authorisation (e.g. the identity of someone might represent default access to resource, and integrity when used in conjunction with hashing techniques). Where digital signatures come into their own is in the provision of non-repudiation controls. Digital signatures are based on public key algorithms.

Cryptography that is used for **encryption** provides authorisation, confidentiality and data integrity when used for secure MACing. Encryption can be achieved using public key algorithms but most



PKI - Public Key Infrastructure

implementations use private key algorithms because this represents a lower processing overhead.

Digital Signatures

Digital signatures are based on a public key encryption system that uses two keys - one to encrypt, another to decrypt the message. A user wishing to send a message generates a key pair and deposits one key in a public domain while keeping the other key private.

The user creates a digest of the message (which is a one way hashing function that is virtually impossible to reverse), signs the digest using their private key and then sends the message and the digest to the recipient.

When received, the signature is verified using the public key - by decrypting the message to produce the digest. The clear text document is then put through the same message digest process and the resulting digest is compared with the one received. Any changes to the clear text message will result in a digest that will not match and, therefore, the message's integrity is protected.

Establishing the identity of two parties who may be thousands of miles apart presents a problem in the world of electronic commerce. If public keys are kept in the public domain it could be difficult to be certain that the public key is the right key and not one that has been substituted by an impersonator. To overcome this problem Trusted Third Parties (TTP) are used. These provide a service where public keys can be stored and managed centrally on behalf of the community.

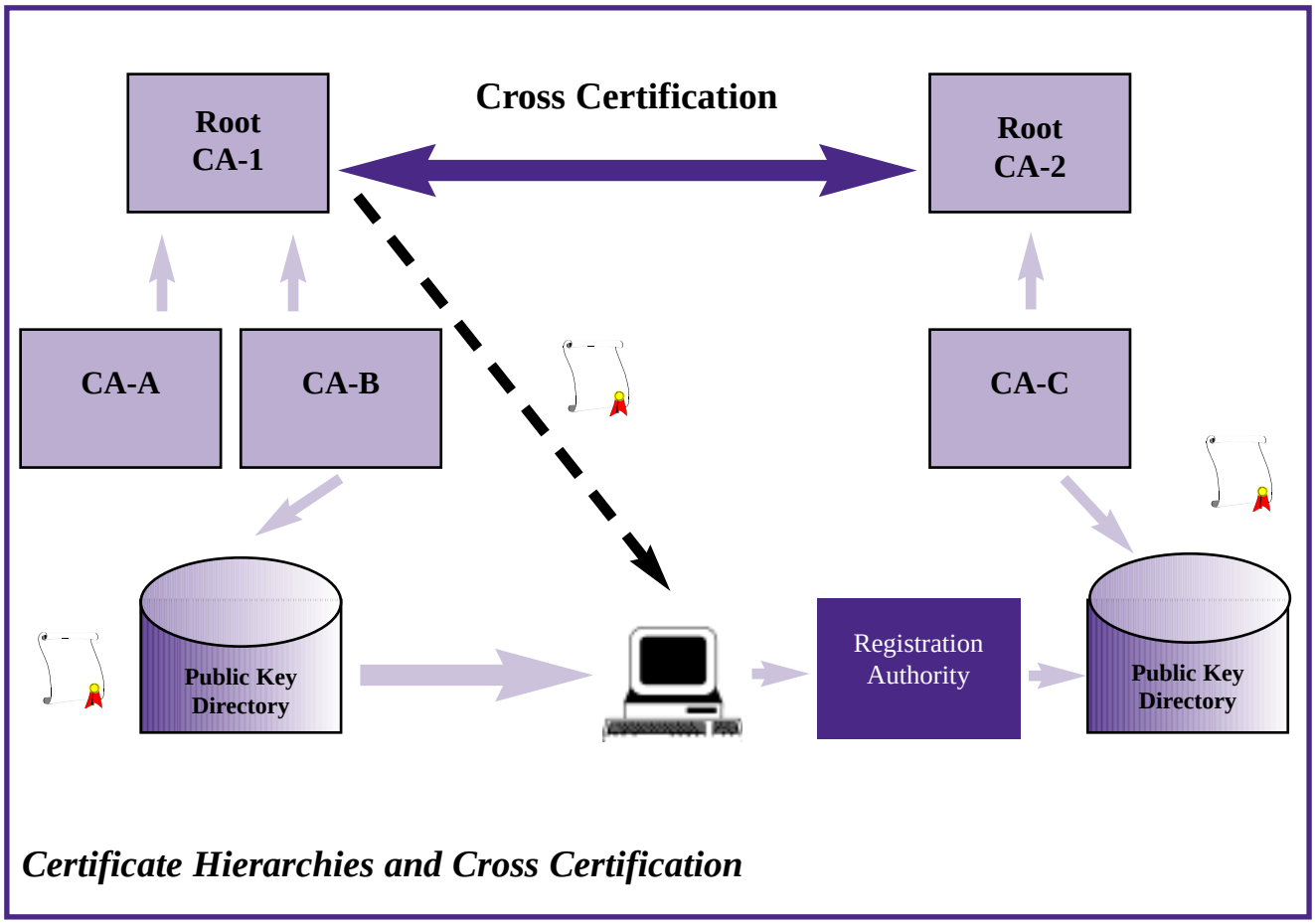
Public Key Infrastructures (PKIs)

A Public Key Infrastructure (PKI) makes use of TTPs called Certification Authorities (CA) who can vouch for a public key by binding it to its owner in a digital certificate. This certificate is digitally signed by the Certificate Authority and deposited with the key in a public directory.

When a user wishes to verify a signature, both the public key and certificate are retrieved from the directory. The public key is then validated by verifying the CA's signature on the certificate (using the trusted CA's public key which will already be known or securely accessible). Because the CA is an entity that everyone can trust, a user wishing to verify the signature of a message knows that the public key received is certified and that this certification can be checked.

In large communities (e.g. international communities) it might not be practical for every user to trust a single or every CA. A user may therefore receive a signature that is not verifiable. To solve this problem, CA hierarchies (where CAs authenticate other CAs and issue what are called CA certificates) can be accommodated in a PKI.

In this situation, a user wishing to verify a signature retrieves the signature and certificate in the same way. Since the CA's signature on the certificate cannot be verified, an attempt to verify the signature of the CA that certified the certificate



Certificate Hierarchies and Cross Certification

issuing CA is then made. This process is continued up the hierarchy until successful or finally rejected.

The locating and verifying of the certificates and signature is known as a certification chain. How far through the chain a signature checking system needs to go depends on the level of trust that is placed in each of the CAs. To reduce the chain and processing overhead, cross certification can also be implemented.

It is worth noting that the CA is responsible for obtaining the necessary credentials it needs to certify a public key. In a large community this may be delegated to another entity known as a Registration Authority.

PKI Issues

There are, however, a number of issues with PKI that still need to be addressed. No one knows whether the current version of PKI will work. Although public key technology has been around for over 20 years, a full blown PKI has not yet been tested outside of a controlled environment. Furthermore, digital signatures may facilitate proof of identity but they are not proof in themselves. They only prove that the person signing the digital signature had access to a particular private key that happened to be signed by a particular CA. Unless a private key can be generated and stored in such a way that it can only be used by one person, the entire process can be suspect. For instance, a PC may not be good enough for storing keys because the rush to get new technology to market often means that they are released without independent testing and are full of bugs. For example, it is conceivable that Trojan horses in the form of Java or ActiveX programs find their way into a PC where they lie in wait for sensitive information that can be forwarded to an attacker.

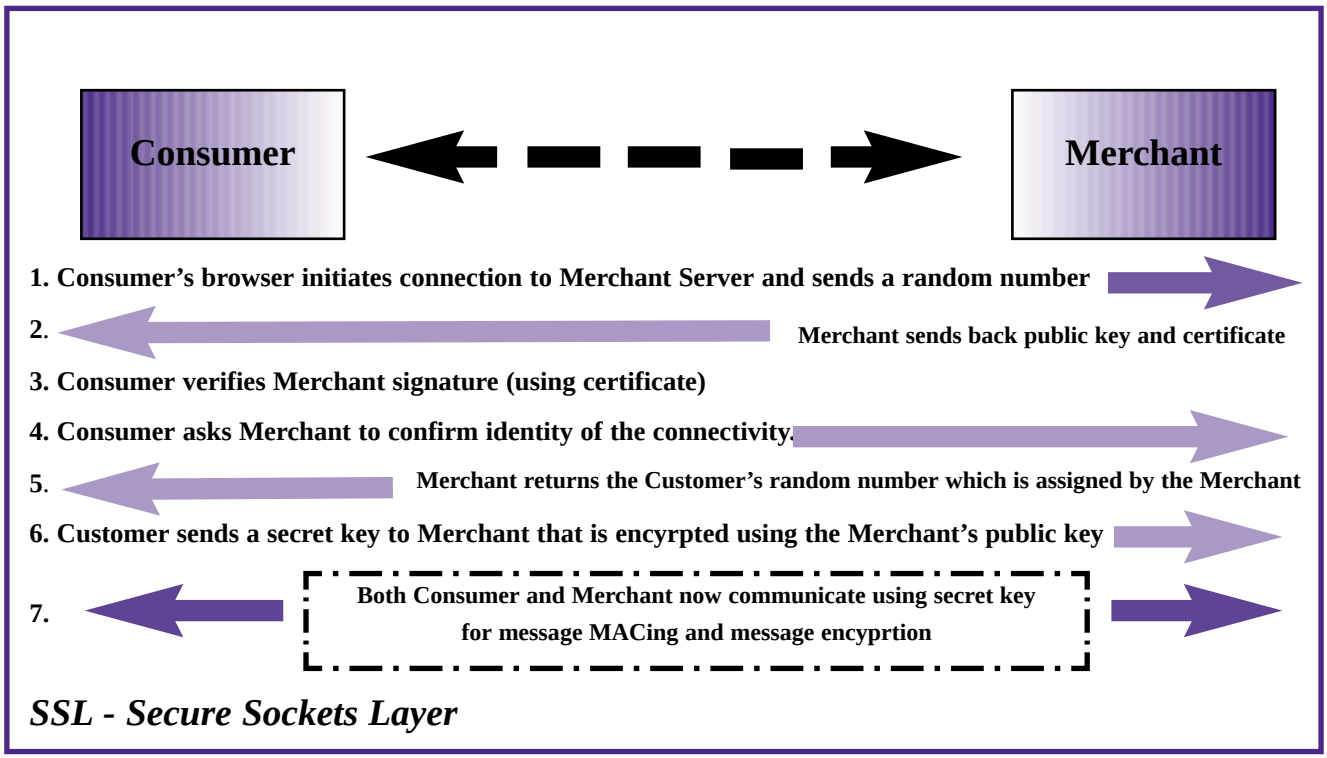
Payments in an Electronic Age

Another area that is receiving quite a lot of interest is payments. Some of the technologies under development and discussion are Secure Sockets Layer **(SSL)** and Secure Electronic Transaction **(SET)**, both of which provide secure solutions for Credit Card transactions. Another payment system that has recently been making the headlines is **Digital Currency**. Digital Currency involves tokens or values expressed in a digital form. This area can be sub-divided further into **Stored Value Cards** e.g. Mondex and **Electronic Cash** such as eCash and Cyber Coin.

Stored Value Cards have evolved from existing electronic funds transfers - such as pre-paid phone debit cards - and their principal function is portability. Stored value cards are more acceptable in Europe than they are in the US and are more popular than electronic cash.

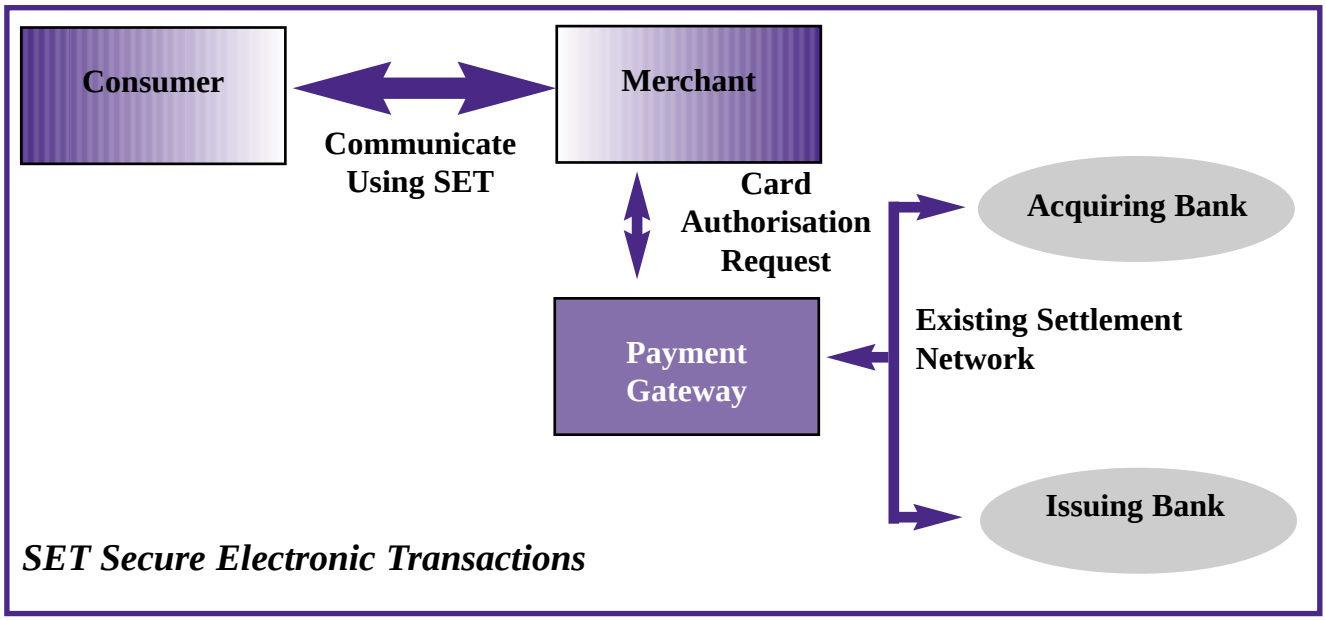
SSL and SET

Whilst electronic cash is being developed, and it will take some time before there is a widely used infrastructure for its use, the immediate developments are SSL, the current protocol that goes some way to provide reasonable assurance in the interim, and SET, the up-and-coming all sophisticated protocol for credit card transactions.



SSL - Secure Sockets Layer

SSL is a general-purpose cryptographic protocol operating at the transport layer of TCP/IP where it provides a secure two-way communications channel. Netscape developed it in 1994 for use in its Netscape Navigator browser. It works by establishing a two-way handshake between the server and the client using digital signatures and



certificates. This handshake also includes steps for exchanging a secret key that is used for providing the actual encryption (confidentiality). Data communication between the client and the server is typically provided using 128 RC4 bit encryption for US server/clients and 40 bit for non US Servers or clients.

The SSL module is invoked through the use of a special URL prefix. For example, "https://" is used to establish an SSL encrypted HTTP connection. The downside of SSL is the performance degradation caused by the public key encryption and decryption that is required during the initial handshake and the lack of real authentication of the cardholder.

Mastercard, Visa and others are developing SET. Its aims are both to provide confidentiality and authentication of the parties involved and to provide a mechanism for payment for goods and services. SET is a solution for sending encrypted credit card numbers over the Internet and, although it is being tested in a number of European countries, it is still very much under development.

There are three parts to SET

✦ *The Wallet* - Software that resides on the customer's PC. This provides the interface, the encryption and decryption services (and the signature and the certificate of the card holder)

✦ *The Merchant* - Software that sits on the merchant's Web which holds the Merchant's signature and manages the exchange of certificates prior to a transaction.

✦ *The Payment Gateway* - Software that runs at the Merchant's bank which carries out the decryption of the payment and transforms it into the existing format before forwarding it on through existing channels.

To use SET, a customer's credit card number is stored in the electronic wallet (usually in an encrypted file on the hard disks but it may also be a smart card). The Wallet encrypts and signs the payment details and sends it to the Merchant. The Merchant then signs the payment slip and forwards this to its bank. At the Bank the Payment Gateway verifies the signature of the merchant and customer and decrypts the credit card details, transfers the information into an existing format and sends it on through the existing channels for authorisation. When payments are authorised, the merchant is notified and a receipt is sent back to the customer.

Auditing

Like everything else in EC, auditing in this area is still fairly new. However, Internal Auditors can play a vital role in the development of this new market and help management win the EC battle by facilitating risk management and making recommendations to promote a sound control environment.

The controls are many and varied and, like EC business, are interdisciplinary in nature. To begin, however, auditors can start by determining whether a company has a strategy for its e-commerce business activities and ensures that this incorporates technology and legal issues. The strategy should be supported by an EC marketing strategy that facilitates the management of reputational risk and establishes brand and trust.

Management must also stay on top of technology developments and the risks and issues associated with them. Therefore, auditors' reviews should be encouraged to examine the information gathering and exploitation processes, ensuring that management are always best placed to stay informed and are able to make the right decisions. Finally, with the new developments in the legal system, management must keep up-to-date with relevant law and regulatory provisions and anticipate change in their business processes and procedures to accommodate them. An internal auditor, of course, can assist in this process.

NETWATCH

By Annabel Lane, Nestle Plc

Welcome to what will be the last Netwatch column of 1999. In my journeys through Cyberspace this time I have eschewed the temptation to revisit all those Year 2000 sites or even point you to some new ones that predict the imminent demise of the social infrastructure closely followed by the end of the world as we know it, which I understand is used as an acronym TEOTWAWKI amongst those in the know.

But, I just felt I had to direct you to:

http://www.hartscientific.com/y2k.htm

the unofficial year 2000 site of Hart Scientific. If you are feeling as jaded about Y2k as I am, you'll appreciate this one - it's full of all the things companies probably should say, but daren't. For example, they admit that "our lawyers tell us we can't promise you anything re Y2k", and advise their customers that if their (i.e. customers') own accounting systems don't work after 31st December they are not buying any excuses - they will be expecting payment by hand written cheque! Of course there is a link to their official year 2000 page too, but I liked this one better!

First I am unashamedly going to point you to an old favourite and I am sure your usual port of call on a regular basis, the ISACA London Chapter website at:

http://members.aol.com/isacalondn

It has been updated over the summer break with details of all the forthcoming Chapter meetings, all on the theme of the extended enterprise (in case this was the first article you turned to in this issue of Datawatch) [who are you kidding? - Ed]. Pay it a visit and arrange your social life for Thursday evenings!

Now that's out of the way, on to my usual review of sites that have caught my interest over the past few months. The flavour this month is slightly more technical, with a nod to ecommerce and security. There's that extended enterprise theme starting up again….

http://www.dataprotection.gov.uk/

No prizes for guessing what this one is all about! For any of you who don't know the government will be bringing the new Data protection act (1998) into force on March 2000. There's some quite technical stuff on here, but also some more reader friendly articles such as a summary.

This is probably the first area to check out if you are a beginner in this subject, as it gives you information such as who the new Data Protection Registrar is, what her duties are, where she is based and most importantly of all, what the act actually is about. There is also information on your rights as a citizen and your responsibilities as a company - I think a few of us will be looking at this as part of our audits in the near future. When I checked the site out for this article it was in a state of transition, so some of the links weren't up and running fully.

http://www.pgpi.com

With the growth of ecommerce there is an increasing demand for encryption as we transfer more and more information by electronic means. One of the best known is undoubtedly pgpi. This is the official pgpi home page and it caters both for the really technical (yes techies, I know I sometimes neglect you!) with developers' pages, and for the less technical who perhaps want to find out more about it. A good place to start from this point of view is the PGP documentation link which takes you into such areas as frequently asked questions, the history of PGP, and an overview of languages and platforms it can be used on. Personally I take my hat off to anyone who creates something and gets away with marketing it as being only "pretty good"!

http://www.itsecurity.com

This site claims to be an encyclopaedia of computer security and all things to all security people. It

says it is a complete, independent, and free online guide to information security. Its main sections include a tutorial, a security products catalogue, a legal section, a selection of security papers and newsletters, and an extensive glossary of security terminology.

The tutorial contains some useful ideas under its various sub divisions. For example, under the section on access control it warns the reader that password access is not an amazingly secure method of access control and that users normally have to be forced to change passwords and use ones which are not easy to guess. (Welcome to the real world!) It also gives some pointers on password usage such as to change the password after a visit from an engineer, and the sorts of passwords to avoid. The section on Internet security deals with subjects such as IRC, Telnet and FTP as a security risks.

The section on cryptography deals with public keys, PGP, international trading and arms regulations and highlights problems and caveats. All in all the tutorial section is very useful for the less technical person who wants a simple background in security in these particular areas.

There are several other sections to this site, for example, a collection of news articles, legal issues, up and coming events, and a glossary of computer security terms which claims to be the most complete on the net. For example did you know what a cyberwoozle was?? Apparently it's a method of siphoning users' data while they surf. Well I never.

All in all worth a visit, especially for the less technical among us.

http://www.antivirus.com/corporate-home.asp

An anti virus site hosted by Trend, an antivirus software company. Some of the initial offerings on the home page include free anti virus software downloads and some news items about Trend services (the front page of the site is at www.trend.com).

There is also a virus hospital service available whereby you can actually send Trend infected files for virus detection and cleaning.

There is, however, a security section which lists top current viruses "in the wild" and links through to a virus encyclopaedia which gives a lot of detailed information - more so possibly than some of the other sites previously reviewed. It is clearly set out, for example telling the reader what languages the virus is written in, what dates activate it, what its "payload" is, and full details of what it actually does and how it operates.

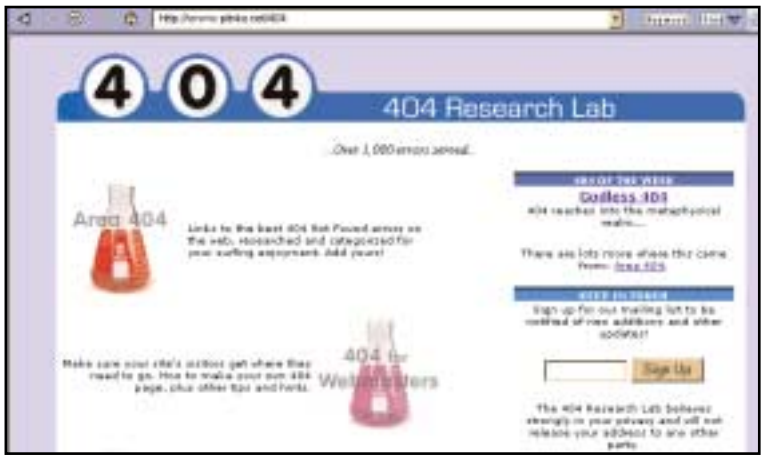
There's also a list of current hoaxes - always useful as my well intentioned colleagues are always asking me about these it seems - plus some tips on avoiding virus infection, such as if you receive an email with an attached file from an unknown source, delete it without reading it.

A useful introduction for the non technical is the virus primer, which talks at a basic level about what viruses are and how they are transferred around, and what their likely life cycles are.

http://www.computingnet.co.uk

Provided by VNU publishing, the people who bring you Computing, an online version of the magazine, with added extras. For example there's a section on Year 2000 (yes I know I wasn't going to mention it again), a "the least you need to know" section, latest news stories, and of course the opportunity to search on key words for articles on particular areas of interest. Ecommerce is a theme that recurs constantly in the computing press, and the times I have looked at this site have been no exception. Useful for keeping up with trends, especially if you don't get the magazine in hard copy format, or for finding background information on particular topics.

http://www.plinko.net/404



"Hey man, he's 404". I have been told that this is now topical techie slang for saying someone isn't quite with it (or eleven pence ha'penny short of a shilling as my granny used to say). For my "coffee break site" of the issue, I have chosen this, a site run by the 404 Research Lab, who claim to be committed to improving the internet experience through the systematic eradication of ugly and confusing '404 Not Found' errors. They think that the 404 error message is of vital importance to the web and wish to "actively improve the quality and helpfulness of 404s throughout the world."

To this end they include links to the best 404 messages on the web, including the coolest, the most informative and naturally, the funniest. So if you wanted to be told to carry out 4 Hail Marys, or grab 404 beers, or that the file you are looking for has been there, done that, and gone on to pastures new, this is worth a look. Also in the interest of improving the quality of 404 messages on the web, there's a section for all you web masters to create and improve your own.

I shall be visiting the London Chapter web site regularly to see if the web master reads Netwatch……

INTERNET RESOURCE LIST

WEB SITES:

http://members.aol.com/isacalondn/
http://www.isaca.org
http://www.cert.org
http://www.auditnet.org
http://ciac.llnl.gov/ciac
http://www.microsoft.com
http://www.alw.nih.gov/security
http://spam.abuse.net
http://www.cauce.org
http://www.acua.org/usu./main.htm
http://www.cl.cam.ac.uk/spam
http://www.rain.org/~lonestar/audit.htm
http://www.rain.org/~lonestar/kits.htm
http://www.iki.fi/liw/mailfilter.html
http://.ntresearch.com
http://csrc.nist.gov/secpubs/unix_security_checklist.txt
http://year2000.com/cgi-bin/y2k/year2000.cgi
http://www.bcs.org.uk
http://www.auditserve.com/frmain.htm
http://www.coactiveconnection.com
http://www.mc2consulting.com
http://www/2600.com/mindex.html
http://2000.jbaworld.com/
http://www.year2000.co.uk/year2000.htm
http://www.open.gov.uk/bug2000/
http://www.ibm.com/IBM/year2000/
http://pw2.netcom.com/~helliott/00.htm
http://www.anao.gov.au/reports.html
http://www.year2000.com/archive/NFaudit.html
http://www.year2000.unt.edu
http://www.year2000.ca.gov/Summit/Contingency/Y2Klinks.asp
http://www.theiia.org
http://www.iia.org.uk
http://www.sophos.com/virusinfo/
http://www.drsolomon.com/vircen/
http://www/ntsecurity.net/
http://www.csrs.nist.gov/welcome/html
http://www.gallaudet.edu/~auditweb/kits.html
http://www.gallaudet.edu/~auditweb/index.html
http://www.year2000.ca.gov/Summit/Contingency/Y2Klinks.asp
http://www.methodware.com/links.html
http://www.first.org
http://www.y2kinfo.com/
http://www.acl.com/audit/audit2.htm
http://www.disastercenter.com/audit.htm
http://www.cica.ca/idea/index.htm
http://www.itaudit.org/
http://www.teleport.com/~jhw/csa/
http://.securityportal.com

NEWSGROUPS

comp.security.announce
comp.security.firewalls
comp.security.misc
comp.databases.oracle.misc
comp.databases.oracle.server
comp.unix.unixware.misc
alt.business.internal-audit
comp.os.ms-windows.nt.admin

CISA

Date of next examination
10 June 2000

Bulletin of Information and Registration now available from the Chapter Office or visit

www.isaca.org/exam1.htm

for a downloadable version or online registration form

Auditing the use of transaction codes - Part One

By Annabel Lane, Nestle UK Ltd

In the first article of this series we talked about some of the risks that are associated with implementing SAP to replace a number of previous systems:

✦ Data now resides in one place only - this potentially means an end to data duplication and hence unnecessary storage costs and the opportunity to protect that data to a greater degree. However it can also mean greater chance of loss and due to the importance of the SAP system for the running of the business, comprehensive back up and recovery techniques will be required.

✦ SAP is a real time transactional system and links together the entire company (or as far as you have implemented modules). We talked about Bert in the warehouse at Fictitious Co Ltd entering damages into the Materials Management module and this being passed through to the ledgers affecting the company's financial position in a matter of minutes or seconds. This clearly gives management the opportunity to have faster and more accurate information (as long as we are getting it right first time) and means no interfaces have to be built, tested and maintained - SAP does it all.

However, this also means that, whereas users were segregated in the past from say, the financial systems, now we are all users of one big system. Limiting users' areas of operation limited the damage they could do. If Bert wrote off ten times as much stock as he should have in error, the chances are that Margaret from Accounts would ring him to check before she put it through into the financial adjustments. Now we don't have that check - controls in SAP are different and we have to adjust to this accordingly. Also, the IT manager at Bert's place of work knows that he only requires access to the warehouse stock system and as long as he is restricted within that system, there is no way he would have the opportunity to be allocated abilities in other areas. But as we've said, SAP changes all that. A user can have profiles assigned to his id from any of the modules implemented. For example, as an auditor I keep telling User Admin that I need read only access right across the modules we use, though some data, for example in the HR module, I would only obtain access to for a particular and limited purpose.

What am I driving at here?? What I am trying to point out is how much easier under SAP it would be to give a user an ability he didn't require, and even which would be extremely undesirable for him to have, for example because it would nullify the proper segregation of duties. All we need is a user administrator who isn't sure of what he is doing and so just allocates the new person in accounts the same profiles that all the others have and a segregated structure could be broken down.

To give an example, most of us would agree that in the area of purchasing, always one where there is a high potential of losses to the company, there are certain abilities we would wish to see vested in different people; eg creating or changing a purchase order, creating or changing a vendor, receipting goods, entering an invoice, initiating a payment run. Given the way SAP works in this area - by matching the invoice when entered to the prices and quantities on the purchase order and goods receipt and approving that invoice for payment - we would be more than a little concerned if we thought someone could raise a purchase order and perform a goods receipt as this would trigger automatic payment. Throw in an ability to create or amend vendors and you have a giant hole in your control system.

In theory it's pretty clear which duties we'd like to see segregated, but how can we identify them in the SAP system? To start with we need to have an idea of how SAP works.

SAP is based on transactional codes which allow a program to be executed, carrying out functions like updating tables, calling up input screens etc. These are the funny combinations of numbers and letters that some of the people in IT enter into the white dialogue box rather than navigate through the menu paths the way the rest of us have to.

SAP is a real time transactional system that links together the entire company.

There are two basic ways to find a transaction code:

1. To find what transaction you are using to perform a particular task, simply click on system in the command line and then status from the drop down menu. Apart from other useful information such as telling you what release of SAP you are running, in the box headed "repository data" the field transaction will show you what transaction this is. For example if you were in user administration viewing users, it would tell you that you were using SUO1.

2. Of course, this being SAP, an alternative way is to interrogate the table that stores all the transaction codes with their descriptions. Either run the option "Display table" or use the transaction SE16. Press execute and for your table name enter TSTC, the master transaction table. In the version I'm running, clicking on the down arrow beside the TCODE box, will result in a very long list of all the transactions available in the SAP system. (It may limit you to the first 100 initially so you'll need to click on the all values button to display them all.) You may notice that transactions appear to be grouped together in the way that they start with certain letters. If we were looking for transactions conferring abilities in the finance and accounting areas, we could pick them out by the fact that they start with the letter F.

Of course that's all very well, but if we are going to review these from a control point of view there are two things we need to know:

1. What transactions do we consider as critical?

2 How do we find out who has them and therefore whether allocation is appropriate?

1. Which are our critical transactions?

Well, really that's up to the company we are auditing; what it's using and what its required level of segregation is. In a small department, for example the ideal level of segregation is not always possible - we may need to consider some compensating controls. I'm not proposing to go through all the modules in this article as it would push me beyond my allocated space (and probably the reader's patience!). So the next issue will contain lists of transactions that would be considered of interest. But since we've talked about the purchasing and supplier payment process, to give an idea, let's consider some of the transactions we might consider important in this area: (Table 1).

TABLE 1.

PROCESS DESCRIPTION	TRANS CODE	
Create requisition	ME51	
Change requisition	ME52	
Release requisition	ME54	
Create a purchase order with an unknown vendor	ME21	
Create a purchase order with a known vendor	ME25	
Release a purchase order	ME28	
Change purchase order	ME22	
Enter invoice	FB02	
Release invoices	MR02	
Payment request	FBP1	
Post outgoing payment	FBZ2	
Create vendor master record	FK01	
Change vendor master records	FK02	

2. Which users have the ability to run our critical transactions?

Version 4.0 contains a tool to reveal this, using the menu path Tools > Administration > User Maintenance > Users > Information > Information Systems. This gives us a screen showing a tree of choices: click on users and then "with critical authorisations". The resulting screen contains a dialogue box for us to enter the code in which we are interested - then pressing enter will give a list of user account names and their profiles.

If you're running a previous version, try entering transaction SE38 or SA38, and then entering RSUSR002 in the resulting program box, then execute. This will give a screen with multiple fields, but the transaction one is about halfway down. Enter the transaction required and the list of user account names and profiles which use it will be displayed.

Next article we'll talk about some of the other modules and list some vital transactions from them, to give a foundation of transaction codes to build on.

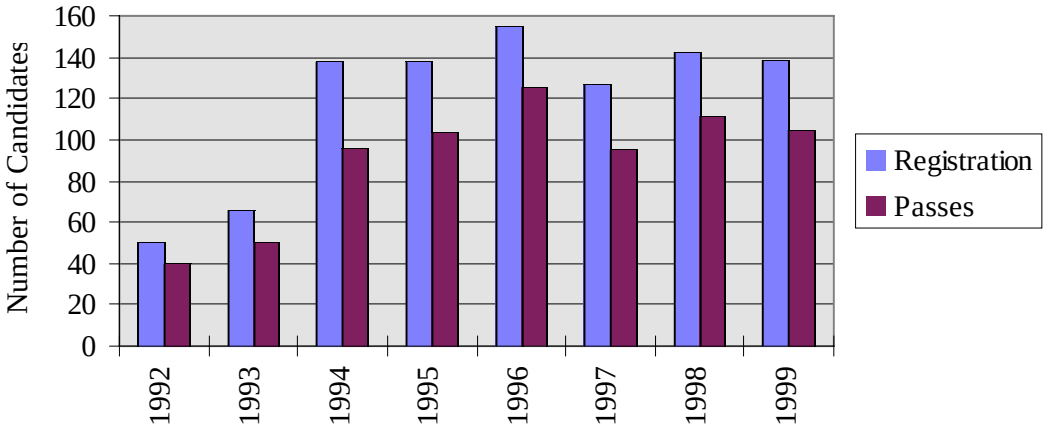
CISA Exam 1999

Congratulations to all successful candidates! Once again the candidates from the greater London area have shown their outstanding abilities with a 75.5% pass rate compared to the overall pass rate of 54%.

This year saw another record with 5,086 candidates registering for the examination globally, and 139 sitting the exam in London.

As the graph indicates the success rate over the last 8 years has been consistently above 74% which is an outstanding achievement.

The graph also indicates the continuing high level of interest of people following our profession in obtaining the CISA designation. There was a peak in 1996 where there was a surge of candidates from the financial sector. Although official statistics are not yet been released, initial analysis indicates that this years candidates were again drawn fairly evenly from across all industry sectors. Within the London area, the majority of candidates were from the big five practices, and from the financial services sector, but commerce and industry were also well represented. This indicates a continuing trend in awareness of the benefits of using IT audit and security specialists in all sectors.



Congratulations to the following candidates who successfully sat the 1999 CISA exams in London.

Mr. Alexander S. Allum
Mr. Benjamin Edward Arnold
Mr. Mat James Bark
Mr. Robert Beaney
Mr. Andrew J. Beard
Mr. Timothy W. G. Ben
Miss Emma Suzanne Biggin
Mr. Mark A. Bolitho
Mr. Ian Bousfield
Mr. Myles Neville Bracey
Mr. Aaeron Brewer
Mr. Stephen Paul Brind
Mr. Ashley Robert Brooks
Mr. Lawrence John Brooks
Ms. Amanda J. Brown
Mrs. Julie Anne Burcham
Mr. Richard Burrows
Mr. Simon J. M. Burrow
Mr. Stephen Ian Butterfield
Miss Diane T. Cannon
Mr. David R. Carlin
Mr. Khalid Chowdery
Mr. Ian Cornall
Mr. David John Crawford
Ms. Amanda Jane Creak
Mr. Graham Creasey
Mr. Anthony Shaun Dench
Mr. Vesselin V. Denchev
Mr. Rakesh Dighe
Mr. Robert J. Dunlop
Mr. John Jeremy Edwards
Mr. Timothy N. M. Ellis
Ms. Jayne Maria Emberson
Mr. Andrew Ferguson
Ms. Sharon E. Foye
Mr. Christopher Gear
Mr. Peter R. Gillespie
Mr. Iain R. Gravestock
Mrs. Alison Tina Grimmett
Mr. Lee Christian Hale
Mr. Daniel C. Halls
Mr. Ben Hammond
Mr. Kevin Paul Handscombe
Mr. Guy Alexander Howie
Mr. Nick Hughes-Davies
Mr. Derek Paul Jackson
Ms. Kirsty L. Jackson
Miss Karen Jaggers
Mr. Stephen G. James
Mr. Ali A. Kazmi
Ms. Laila Pervin Khan

Mrs. Inna V. Kileinikova
Mr. Stephen John Kimber
Mr. Michael C. Kirkman
Mr. Mukesh Kumar
Mr. Ajay Kwatra
Mr. Paul A. Lacey
Mr. Colin B. Levy
Mr. Richard John Lundie-Sadd
Mr. Tsun Wah Lung
Mr. Malcolm MacDonald
Mr. James D. Mahon
Mr. Torsten Mailahn
Mr. Paul F. Martin
Mr. Stuart C. Matheson
Miss Christine Maxwell
Mr. Neil Richard May
Mrs. Pamela Anne McDonagh
Mr. Ray L. McKeown
Miss Angela Jane Medley
Mr. Michael Meli
Ms. Gabriele Friederike Monk
Ms. Margot E. Mouat
Mr. Philip G. Ogborne
Mr. Sujit A. Patel
Miss Clare M. Patterson
Mr. George Doherty Quigley
Mr. Krishna Rajan
Mr. Oscar Francis Remedios
Mr. Oswin Xavier Remedios
Mr. Simon Neil Riggs
Mr. Martin B. Rogers
Mr. Peter Rubie
Mr. Carlos A. Russell
Mr. Leslie R. Samuels
Ms. Maya Shlomo
Mr. Brian J. Shorten
Mr. Andrew H. Simpson
Mr. Christopher John Smith
Mr. David Spaven
Ms. Tina Stanyer
Mr. Richard John Stapleton
Mr. James W. Story
Mr. David M. Thirlwall
Mr. Daniel Tuson
Mr. Ananthasubramanian Vaidyanatha
Mr. Richard Wakeham
Mr. James C. Watson
Mr. Richard E.H. Wharton
Mr. Royston John Whiddett
Mr. David J. Williams
Miss Kirsten L. Williams
Mr. David K. Wilyman
Mr. Paul E. Wright-Anderson
Mr. Andrew John Wrigley

Special Interest Group (SIG) Fraud Prevention

Initial meeting - 25th November 1999

Sanwa Bank Ltd, City Place, 55 Basinghall Street, London EC2

ISACA special interest groups meet informally to discuss specific areas of interest to their members and this note is to introduce a new group looking at the subject of Fraud Prevention. At this meeting we'll be setting out the areas the group wants to address. So if this is a topic you're interested in, come along and, as in the famous quote - "..share what you know, learn what you don't".

The topics could include:

- **E-Commerce is often touted as the safest way to buy goods, but is it the riskiest way to sell?**
- **What are the characteristics of 'electronic fraud' opportunities?**
- **Where do certification and the use of electronic signatures fit in?**
- **Common and not-so-common frauds**
- **Fraud statistics**
- **Detecting and deterring frauds.**
- **Supplier & vendor frauds**
- **Employee frauds**
- **Defences**
- **Behavioural risk assessment**
- **Money laundering**
- **"at risk" business processes**
- **e-Commerce**

The group would be looking to producing an ISACA publication on this subject. This SIG is suitable for internal and external auditors, IT security and e-commerce specialists from the commercial and financial sectors. (even if you just want to get your name on a publication for your cv!)

MILLENNIUM NewsBYTES

By GREMLIN

UK won't follow the US

In July, Y2K Minister Margaret Beckett ruled out any possibility of the UK following the US with a law to reduce the chances of lawsuits arising from non-compliance. The so called US 'Good Samaritan' Act passed into federal law on July 1st (HR775) despite rumours that the Clinton administration would try to block it.

The US Act guarantees that a Y2K disclosure made by a company cannot be used against it in court if a dispute arises. Beckett believes that such legislation would add additional burdens to SMEs struggling to reach compliance. This view has come under attack by city law firm Tarlo Lyons who have expressed concern that the Government has failed to see the merits of such legislation in encouraging companies to be more open in their Y2Kdealings.

The UK is increasingly looking out of step when compared to countries such as Australia, New Zealand and the Philippines. These countries have already implemented protective legislation and Tarlo Lyons is predicting a rash of law suits in the new year as company directors, bound by a duty of care to shareholders, seek to recover damages from non compliant supply chains.

FCO fails to Act

The Foreign and Commonwealth Office which has come under fire for failing to get its Y2K act together, (see Newsbytes passim), received a roasting in July from the House of Commons Foreign Affairs Committee. The committee is pressing for an independent review of the department's Y2K strategy and its overall approach to IT. The Committee believes that the FCO has been handicapped by an inflexible pay and grading system which has failed to take into account the market rate of IT specialists making it impossible for the department to recruit or retain the required IT skills.

Alarm bells on the Committee started to ring when the FCO declared that it would achieve Y2K compliance by "replacing equipment where necessary and through electronic fixes and procedural workarounds".

Boom time for Agencies

With the National Computing Centre reporting that less than one in four companies have negotiated staffing arrangements for the millennium period, recruitment and contract staffing agencies are looking for a pre-millennium profit boost. Many have already been trawling through their database of contractors to determine who is willing to work over the holiday period in order to meet the anticipated panic reaction from companies in the late Autumn.

For those expecting to rely upon contract resources, the news is mixed. While 80% of contractors surveyed by contract staff agency DP Connect were willing to forgo the parties, they will only do so for a substantial cheque.

The NCC is warning companies to plan now or face stratospheric costs for contingency staff later in the year.

But maybe it's all hype?

Mike Hinden, IT Director of Johnson Fry Holdings, a Financial Services sector company, begs to disagree with the predominant assumptions of staff shortages. "Three years ago, industry was being told that unless the experts were called in mmediately, by the end of 1998 there would be no consultants and technicians left to solve Y2K problems," Hinden adds "I am being bombarded on a daily basis by offers of help from consultants, technicians, and HR agencies." Frank Coyle, IT director of the newsagent group John Menzies agrees, commenting that recruitment agencies have assured him that there are plenty of staff available. Michael

Khan, IT director at 'Specsavers' certainly hasn't been paying over the odds for contract staff, nor has the company needed to resort to loyalty schemes to hang onto IT professionals. Russell Clements, MD of recruitment agency 'Computer Futures' comments that "….there has been a tailing off in demand for Y2K skills, but it's not true to say it was always hype. There was a time when there was a genuine, huge demand. People were paying wild salaries, so the demand and supply equation must have been in favour of the sellers." Clements adds "There's still a big demand for Cobol and assembler people. Some of the larger companies still aren't in as sanguine a mood as they might indicate."

So there you have it!

Boom time for IT?

Well once the planes have fallen out of the sky onto the debris of the financial services sector, will there be any good news to ease the agony of the New Year hangover? According to ICL, the conventional myth of a shortfall in IT expenditure next year is plain wrong. The predictions of the gloom merchants have been based upon an assumption that so much will have been spent on fixing the Y2K bug that there will be nothing left in cash strapped budgets for new development work. Jane Burns, ICL's marketing manger sees the landscape rather differently, "We expect to see the floodgates open early next year as companies say "OK we're now ready to start the real work of the business." Burns believes that there is a backlog of IT development work which has been shifted to the 'back burner' as corporates have concentrated on their millennial problems. Once this problem is resolved, she confidently predicts an upsurge in demand for knowledge management and e-commerce applications.

UK Government facing embarrassment

The Government could be heading for a big shock unless it heeds warnings from independent bodies that the UK is not prepared for the Y2K problem. Yes, Robin Guernier has been on the 'warpath' again following a Government select committee report into the readiness of Britain's beleagured public services.

"The government has handled Year 2000 badly and the political issue is bound to come to the fore soon. It is going to get criticised when things go wrong, especially as ministers continue to say that everything is going well. How can they continue to reconcile the government view that it will be alright on the night when all independent reports say the opposite?" questioned Guernier.

The committee report, entitled 'The Millennium Threat', says it is disappointing that central government, and in particular the emergency services, have failed to sufficiently tackle the bug.

Despite a significant and costly programme of work "there is still much to be done before all key systems are shown to be millennium compliant," claims the report.

Police forces and fire brigades are accused of not being "as far down the track as they should be".

Responding to the allegations, Ken Jones, assistant chief constable at Avon and Somerset Police, said: "I'm certain the report is based on old information. The tension that's been raised is misplaced because all forces but one have been coded as amber - which means that while there is some risk, there are containment plans in place to reassure people that if nothing else is done everything will be OK."

Action 2000 agrees, claiming a great deal of progress has been made since the committee started its report. But Guenier claims the report's findings are not a new discovery, as they have already been stated by a large number of august independent bodies, including the Audit Commission.

IT budgets hit by millennium effect

European IT spending will remain flat throughout next year, according to one recent survey - but another analyst house is claiming that budgets will continue to grow as more money is devoted to EMU and e-commerce projects.

Research conducted by US investment bank Salomon Smith Barney (SSB) found that European IT directors are not expecting to increase their IT spending next year. In comparison, budgets leapt by 29 per cent this year.

SSB surveyed 46 IT directors in Europe's leading companies. Niall MacLeod, equities strategist at SSB, said: "Spending this year was partly bumped up by year 2000. It was only 12 per cent of budgets in 1998, compared with 17 per cent this year." But Stephen Minton, senior analyst with IDC, described the findings as "nonsense", and claimed: "Our research shows that IT spending will be fairly steady throughout the next five years, and we forecast growth over the whole of Europe at nine per cent in the year 2000, and over 11 per cent in the UK." The mood is optimistic in the reseller community as well. Earlier this month, Computacenter CEO, Mike Norris, noted that his company's results for the first half of 1999 had felt the impact of Y2K, but expected a turnaround next year.

He said in a written statement: "There has been some evidence of a slowdown in the corporate market across Europe as the millennium approaches. However, we believe there is significant pent-up demand in our customer base which will be released next year."

IDC's Minton agreed with that assessment. "We see a refocusing of spending on different areas, resulting in drops in certain hardware segments and much higher growth in services and software. But the Y2K effect is not going to bring down IT spending overall, because once Y2K is over, there's EMU and ecommerce and lots of other factors keeping the market buoyant," he said.

'Irresponsible' vendors accused of posting false Y2K data

Software vendors are damaging the business community by constantly changing the Y2K compliance information on their Web sites, according to Action 2000.

It paints a very dismal picture," said Gwynneth Flower, director of Action 2000. "One would assume that if you'd followed the advice given on the company's Web site you'd be protected. It has got to the point where it's quite unreasonable."

Flower believes the software industry "fudged it" in the beginning, putting up erroneous compliance information that later needed revision.

Alison Ryan, public affairs officer at the Consumers Association, said: "Consumers have less than a month until 9/9/99 and only a few months more to the year 2000. Removing these Y2K fix-its and guarantees from Web sites is really irresponsible."

"The nearer it gets to the year 2000, the more unreasonable it is for a product to be non-compliant. Software doesn't have a life of three months," she added.

Microsoft's year 2000 manager, Vaughan Smith, said: "Customers must determine their own level of compliance according to how they use the software."

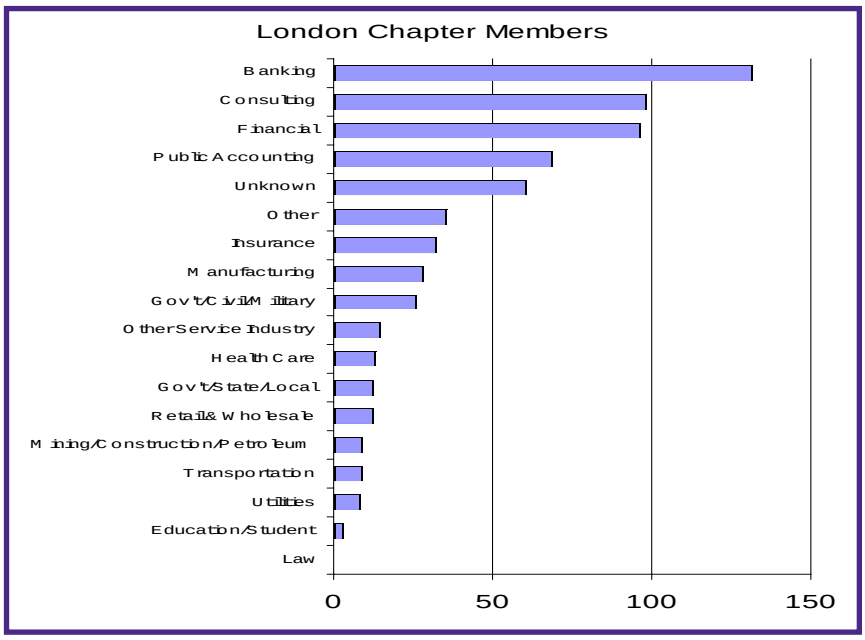
He added that 98 per cent of Microsoft's products are compliant. The changes in status, he said, reflect the fact that Microsoft customers are continuing to call the company's attention to non-compliant uses of the software. Microsoft is then obliged to add this information to the site.

Smith said that the company was planning to contact 60 million customers in September and October to remind them to check the Web site to update themselves on the compliance levels of their products.

Chris Turner, European project director for Unisys, had sympathy for Smith's view. "An awful lot of organisations are undergoing extensive testing of systems," he said. "It's hardly surprising in all the various environments that unusual errors are arising and being reported back to the manufacturer," he said.

Membership News
By Kamal Khan

I am very pleased to report that London Chapter now has over 650 members, the highest number ever.



While Banking/Finance and Consultancy are the biggest users of IS Auditors, we seem to be spread over almost every sector of the economy. However, there are still a lot of members who haven't yet got CISA qualification (around 300 about 45%), so if you haven't yet taken the exam, 2000 could be your year!

It occurred to me that members who cannot make it to the monthly Chapter meetings would never get to meet other IS Auditors as there is currently no mechanism to enable this. If you are interested in getting in touch with other auditors in your area, please write or send me an email giving me permission to do so, and I could put you in touch with others in your area or sector who have expressed a similar interest.

Controlling and Auditing Electronic Commerce

By Keith Osborne

The last two years have seen a tremendous expansion in e-commerce and with this, the hope of financial reward - but at what risk? In this first article of his series Keith Osborne gives an overview of controls in e-commerce.

The explosive growth in e-commerce

The last two years have seen an explosive rate of growth in e-commerce, as well as other networked facilities, such as the use of e-mail and information dissemination through web technologies. The particular characteristic of such facilities that is of most note is that it is not its use within organisations that is so remarkable, but its use between organisations and individuals. This is rapidly leading to the "Networked World", where more and more individuals and organisations undertake business and social functions electronically.

Why has there been such a rapid growth in e-commerce? There are several answers, but the main ones include:

- Speed
- Convenience
- Cheapness
- Availability
- Use of current technology
- Peer-group pressure

The issues of control

The key issues for organisations in the use of e-commerce involve both the nature of controls in e-commerce systems, and the ability of those organisations to have a sufficient and appropriate framework of controls. For the control community - Information Security practitioners and Information Auditors - the issues centre on their ability to understand, evaluate, implement and test such controls. The pace of development of e-commerce, and the potential and risks of abuse and fraud is such that these control and audit requirements need to be urgently considered.

E-commerce is not just about the technical issues involved, but is a combination of this technical infrastructure with both the business requirements of trading electronically, and the associated management and procedures. This is a holistic approach to e-commerce, and, from a control perspective, it is imperative that this is the approach taken.

This article will be more concerned with the control issues than the underlying technical infrastructure, but it is important to remember that these three aspects are interdependent - each aspect is dependent on the others. The effective control of e-commerce depends on the total framework of control, not just on one of the component parts. For example, it is not sufficient to consider just the technical infrastructure - to achieve adequate control it is also necessary to look at the business justification for the use of e-commerce, as well as how its use is managed.

The business requirements for trading electronically

The first consideration from both business and control perspectives is to ask why should an organisation trade electronically. It is not sufficient to answer with "because it's there". There need to be more compelling reasons, some of which were listed earlier. From a control perspective, as well as from sound commercial approach, recognition of the risks associated with e-commerce as well as the benefits to be gained, needs to be investigated and evaluated.

Looking at just three of the commonly perceived benefits of e-commerce shown above, it is easy to see some of the downsides:

Benefit	Downside
Speed	Loss of details
Convenience	Loss of rigour in procedures
Cheapness	Trading unnecessarily

As with everything, the rosy picture painted by the benefits is only part of the story, and both Information Security practitioners and Information Systems Auditors will want to be able to see a carefully evaluated "E-commerce P&L".

Management and procedures

Once a decision has been taken to trade electronically, then it is essential that a robust scheme of management control is exercised from the outset. This means that the procedures should be developed and tested before e-trading starts: as with every system of control, it is much

harder to bolt controls on afterwards. These aspects will include the following:

- ✦ Approval
- ✦ Authorisation
- ✦ Authentication
- ✦ Accuracy
- ✦ Timeliness
- ✦ Maintenance of Integrity
- ✦ Completeness
- ✦ Logging/audit trail
- ✦ Verification

As can be seen, some of these are also specific functions of the technical infrastructure.

For Information Security practitioners involved in the management of security, key considerations will be the overall design of the control framework. The design of this control framework will need to consider the appropriate mix of the four types of controls, which are:

- ✦ Supportive
- ✦ Preventive
- ✦ Detective
- ✦ Corrective

Additionally, Information Systems auditors will want to ensure that the control framework is appropriate and sufficient for them to undertake e-commerce operational reviews.

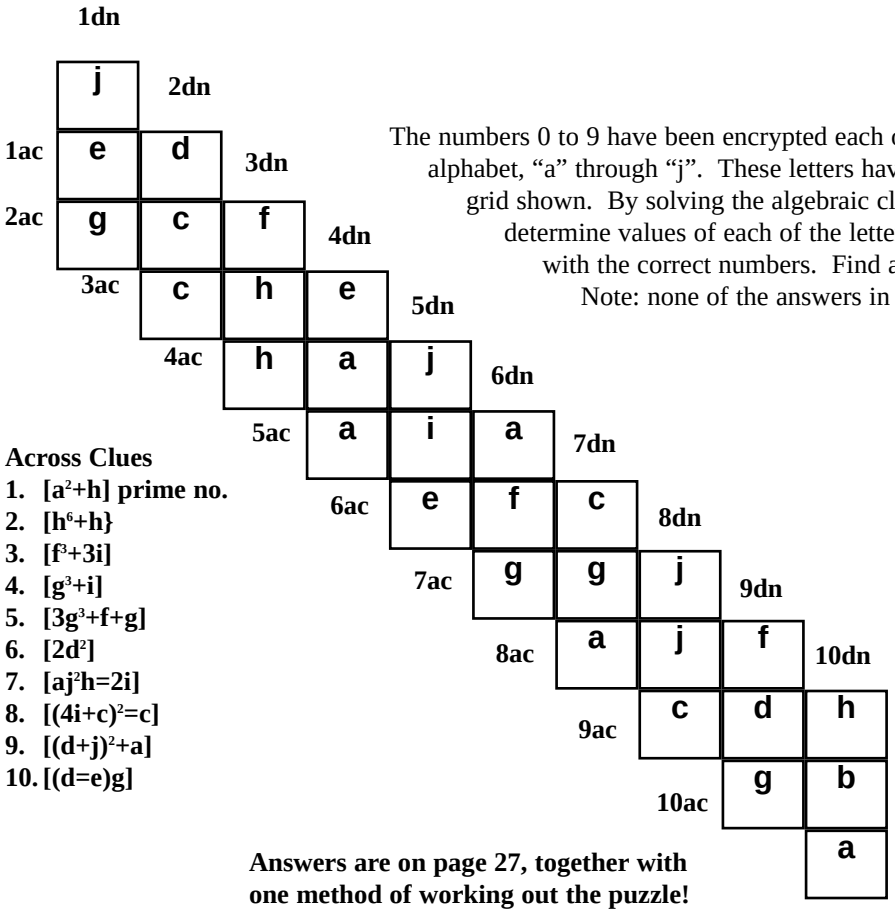
In the next article I will take a look at Abuse and Fraud in e-commerce.

Keith Osborne is Principal, Information Security with ICL. He is actively involved in many aspects of commercial Information Security.

His involvement with ISACA has been considerable: he was involved with the EDPAA Northern chapter from the beginning, and was that Chapter's secretary for two terms.

He can be contacted on 0118-935 9751.

Encryptogram by Puzz



The numbers 0 to 9 have been encrypted each one allocated a letter of the alphabet, "a" through "j". These letters have been correctly entered into the grid shown. By solving the algebraic clues below, it is possible to determine values of each of the letters and replace the grid's letters with the correct numbers. Find also the connecting "theme".

Note: none of the answers in the grid begins with a "zero".

Across Clues

1. **[a^2+h] prime no.**
2. **[h^6+h}**
3. **[f^3+3i]**
4. **[g^3+i]**
5. **[$3g^3$+f+g]**
6. **[$2d^2$]**
7. **[aj^2h=2i]**
8. **[$(4i+c)^2$=c]**
9. **[$(d+j)^2$+a]**
10. **[(d=e)g]**

Down Clues

1. **[$(a^2+h)(gf+e)$]**
2. **[(hg+c)(2gh-c)+c]**
3. **[$h+h^2cig$]**
4. **[$(2f)^2$]**
5. **[(if+g)(if-g)]**
6. **[{$c^4+(h^3+c)$}+h]**
7. **[c^3f^2]**
8. **[ch^2g^2]**
9. **[i^4+jd]**
10. **[$a^2(a^2+h)$]**

Answers are on page 27, together with one method of working out the puzzle!

Security of Telephone Networks

By John Kirby

All telecom and IT managers know that there are hackers out there and most have taken detailed steps to protect their data networks.

Most are familiar with Firewalls and know that a modem and a network card in the same PC invites the attention of the professional or amateur hacker.

Despite the length of time that we have used digital switches to operate our telephone networks not so many of us are conversant with the tricks employed by the telephone hacker or "phreaker" as they have come to be known. This article relates some of the experiences of Secure Dimensions Limited, a company which specialises in the security of voice and data networks.

Toll Fraud

We all know that internal toll fraud can happen. Many employees use the company's telephone for private calls and most companies will have a policy for what is acceptable in this area. The real goldmine for the telephone hacker is to find a switch which the Direct Inward Subscriber Access (DISA) facility enabled. This allows an employee to dial into the company switch, dial a code and a password, and then dial out on the PSTN enabling the company to pick up the cost of the call. Should the password become available to a telephone hacker he can route many calls through that company's switch before the fraud is identified. Some firms have suffered losses of over £250,000. In a recent year known fraud cost British business some £60m but the actual figure, including the undeclared fraud which was absorbed as being too embarrassing to reveal, is estimated to have been in excess of £300m.

Corporate Embarrassment

Any action that gives an impression that a business is not totally professional will have an adverse effect on that firm's image. Imagine the re-action of a potential client if your voicemail message had been modified to suggest that a competitor would do the job better. This can be easily achieved if proper protection has not been programmed in the remote access capability of the voicemail system. Just to admit to significant toll fraud is also deeply embarrassing and is the reason why no companies have been named in this article; it is also the reason why the true value of telecoms fraud is almost impossible to compute.

Loss of Service

All modern digital switches rely on remote access to their maintainer for regular updating of the configuration of the software. This reduces travel costs and allows a timely response to a technical problem that is too complex for on site staff to deal with. The modem linking the switch to the PSTN is also a vulnerable point and if the appropriate password controls are not in place then the entire system can be switched off remotely. It is worth considering just how important the telephone system is to your company. If you consider that it is a critical resource then independent advice on the security systems that are in place should be sought; it may be more convenient for your maintainer to leave a less than fully effective protection in place to ease their access when required.

Phone Tapping and Eavesdropping

The modern digital switch is a gift for those seeking to acquire information illegally. Access to the maintenance terminal would enable a hacker to automatically set up a conference call each time the Chief Executive is called; he would not be aware that a third party was listening on the line and no anomalies would be detected if the phone was swept for listening devices. Corporate intelligence information fetches a high price and the damage to the targeted business could be catastrophic.

The latest digital telephone exchanges may have some or all of the following devices attached to them. All may be controlled remotely through modems and therefore carry a risk of external unauthorised access:

· Maintenance Terminal
· Call Logger
· Voicemail system
· Call Centre Software

In addition DISA and customised links to cellular telephone systems provide additional external access. The switch manufacturers will set up their switches to meet the standard configuration modified by any special features that the client wishes to specify. They will not be liable for any toll fraud on a switch which can be re-configured by their client.

In order to identify the risk areas in your organisation's telephone systems you should consider a telephony security assessment to audit the configuration of your switches and identify all means of external access. The resulting report of recommendations for protecting you from toll fraud, corporate embarrassment, loss of service and eavesdropping could be the most cost-effective insurance policy that you ever invest in.

The Security Column

By John Hunter

Well it had to happen, in July CdC released the Trojan 'Back Orifice 2000'.

It's got quite a number of new features, but the most important one is that it will run on Windows NT. So all you who didn't bother reading my article on the original BO some months ago because it was only for the Windows 95/8 community will have to dig up your old copy of Datawatch for the details behind this little gem. I'll restrict my comments to Windows NT in this article, but remember it wins on W9x as well.

As before, the program is in two parts - a client and a server. Run the server on one machine then any other machine on the network can run the client program to have direct control over that machine. One main difference in this new version is that it is said to feature strong encryption - so can be used securely by a network administrator without worrying that some hacker is trying to get in……if only!!!! I suppose that there are some out there who would load a hacker's tool on the basis that the author says its ok (but would they be a Datawatch reader?)

The program has been released with its source code 'to encourage further development by the security community' so we can expect many more derivations of this in the coming months.

It is very difficult to detect Back Orifice 2000 running on a machine because it is so highly configurable. By default, it will install itself in your Windows system directory as the file UMGR32.EXE and a Windows NT service called "Remote Administration Service." These are the default names and can be changed.

To remove the server, the program recommends that you connect to the server with the client, and go to 'server control', and run the 'shutdown server' command with the 'DELETE' option. If it's a password-protected installation and you don't have the password, or you didn't mean to run it, you'll have to hunt through your registry and startup groups to delete the appropriate registry keys , see table 1.

It is quite a powerful tool and there is even an add-in that sends the server screen as a streaming video to give you a realtime view of the server.

Talking about things running that you don't want to, do you know how many different places can be configured to start a program? For those who don't, I thought that it would be useful to list them, see table 2 on page 26.

There is quite a nice shareware program, 'StartEd' which goes examines the Registry and Startup folder and win.ini listing files which your computer auto-starts. It is available from www.alberts.com. However, It doesn't search the two .bat files.

As I was putting this list together, I started to think about the current proliferation of virus infected emails. I couldn't help wondering how long it will be before all ISPs do the right thing and offer to scan and disinfect emails before they are passed on to the user.

Continued on page 26.

Table 1

Edit the Windows registry using REGEDIT.EXE

Delete the UMGR32.EXE key from:

HKEY_LOCAL_MACHINE/SOFTWARE/MICROSOFT/WINDOWS/CURRENTVERSION/RUNSERVICES

Next, reboot the system and delete the file 'UMGR32~1.EXE'. It defaults to being in the %system%/SYSTEM32 subdirectory, but you should use 'Find' on all hard disks to make sure.

Employment Security

By Adrian Simpson

Unemployment has recently fallen to 1.2 million, at 4.2%, its lowest level since 1980. The trend is continuing downwards. Should this provide you, a computer auditor, with greater job security? Whilst the obvious answer is yes, the more considered one is perhaps only maybe.

At the beginning of this year, when, in anticipation of a recession, the hatches were being battened down, I do not recall any computer auditors being made redundant. "Sorry, business is bad, we have to let you go", unlike the early 1990's, did not become a common refrain. Most companies have come to appreciate that computer auditors are difficult to recruit and are loath to make them redundant for short-term commercial reasons.

At the moment, putting asset price and Y2K concerns to one side, the economic picture is positive. However, whilst the relationship between employers and employees may appear benign, there are few grounds for taking job security for granted. In recent years and 1999 has been no different, there has been a stream of both general and computer auditors being made redundant. The reasons are varied, but usually involve reorganisations, downsizing, takeovers, outsourcing or even new Heads of Audit with new ways of doing things that do not always include the existing audit staff. Employment relationships have changed and have undermined job security that was once taken for granted. These changes reflect the need for companies to regularly reinvent themselves, to grow and evolve in a way that fifteen years ago was not expected. As a consequence, computer auditors should be aware that they cannot rely on a relationship with a single employer to provide them with security.

Computer auditors when considering their careers should think not in terms of job security, but in terms of employment security. This is not an exercise in semantics but a recognition that many computer auditors reading this will, at sometime during their career, be forced into the recruitment market at a time they might not otherwise choose. Their job security will have proved to be illusionary. The objective, therefore, is to ensure that you have a suite of qualifications, skills and experience that will be in demand from the widest possible number of employers. This is particularly important as many industries such as banking, insurance and retailing, that have historically employed large numbers of computer auditors, are continuing to rationalise. Whilst the total number of computer auditors employed in the economy may not be in decline, the number of internal audit departments and therefore potential number of employers is. In some parts of the UK this has resulted in perhaps only a handful of internal audit departments being within commuting distance of a computer auditor's home base.

The demand for computer auditors is going to continue to grow

An important selling point on any computer auditor's CV is not only their qualification, skills and experience, but the impression that they are familiar with change and the challenge of working in new environments. In these terms, it is a paradox that those computer auditors who have enjoyed long term job security, have, should it ever be required, the least employment security.

Although most computer auditors who have been made redundant during 1999 have found new positions with varying degrees of ease, some continue to find it difficult. These have included the older, less well qualified or those who live away from major commercial centres. The contract computer audit market has grown in the last ten years and during this time it has almost invariably provided employment for otherwise redundant computer auditors. It has allowed them to continue working whilst they searched for permanent work.

Curiously, however, in spite of an economy that is growing and generating jobs, the market for both contract and permanent computer audit positions has been subdued in recent months. This is most likely a temporary aberration and is connected to Y2K. Whilst Y2K provided a fillip to the demand for computer auditors during 1998 and the early months of 1999, many companies have now suspended the development and implementation of new systems until next year. Systems development probably constitutes the largest element of many computer auditors' work and its temporary curtailment will subdue demand for their services probably into the second quarter of 2000. By then, no doubt, many companies will be clamouring for computer auditors as a backlog of new developments is initiated.

I have little doubt, barring some unforeseen economic malaise, the demand for computer auditors is going to continue to grow. However, anyone who takes their job security for granted, without considering the demands of the wider employment market, could find themselves sitting at home for rather longer than they imagined.

.... continued from page 24.

I recently came across one ISP, Star:

(http://home.star.co.uk/index2.html)

who offer to scan all e-mail passed to and from its customers as part of their free service. They use three of the more popular virus detection tools to screen every single e-mail and attachment. Come on the rest of you!

Finally, e-commerce is ISACA's theme for this year and fraud is going to get an awful lot simpler as companies jump on the bandwagon without proper controls in place. If any of you would like to get together to start a discussion group on this subject, I'll be starting a SIG this autumn and would be very pleased to see you - look for details on page 16.

Table 2

1. Autoexec.bat

2. C:\windows\winstart.bat - This might be a new one for some of you - It is like autoexec.bat, but runs as Windows starts.

3. Win.ini
[windows]
load=
run=

4. System.ini - Only 2 entries are allowed:
[boot]
Shell=Explorer.exe trojan.exe

5. Files in the Startup folders

6. Registry Entries:
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices]
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce]
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce]
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce]
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices]

7. C:\windows\wininit.ini - Often Used by Set-up programs. When it exists it is run ONCE and then deleted by Windows.

An example wininit.ini file might be:

[Rename] notepad.exe
NUL=c:\windows\notepad.exe

This example runs c:\windows\notepad.exe, then deletes it.

10 Years Ago

From EDPAA DATAWATCH, VOL. 7, DECEMBER 1989

"In a [press] article concerning the problems of enforcing new laws on hacking, the question of defining exactly what is a computer appears once again ".... technical definitions of a computer are too difficult to define and are likely to become outdated too quickly if defined." Or, back to someone's comment at one of our recent meetings about having your hands chopped off for hacking into an automatic washing machine. In the same article, The Data Protection Registar states "I believe that it would be wrong to criminalize those who have no criminal intent and who create no hazard". No comment.

Would you lie to a Computer!

Also in the US, researchers have concluded that people interviewed for jobs are more likely to tell the truth to a computer than to a personnel manager. This is because, they say, people will tend to give the answers that a human interviewer wants to hear. A further factor is that some interviewees really think that the computer is parr of a major network capable of verifying their responses! There is some hope though, because some people who took part in the trial - potential management trainees, felt resentment at being interviewed by computer.

EFT Systems

Did anybody also notice, in the News Roundup in The Times recently the story of the Bank, an unnamed member of CHAPS, that duplicated its payments and lost 2 billion in 30 minutes. The article went on to suggest that most of the money had been recovered and that the error was traced to a software design flaw.

Answers to Encryptogram puzzle on page

								8
							1	9
						7	2	6
					2	3	1	
					3	4	8	
				4	5	4		
			1	6	2			
		7	7	8				
	4	8	6					
	2	9	3					
	7	0						
	4							

Values: 0 = b; 1 = e; 2 = c, 3 = h; 4 = a; 5 = i; 6 = f; 7 = g; 8 = j; 9 = d

Theme: The central diagonal of the grid is in sequence

One method for solving the puzzle:

From the pre-amble, none of the answers begins with a zero, so from observation of the grid and the clues, **0 = b**

Using the clue 4 down, the only 3 number squares ending in the same two digits are 144, 400 and 900, but 0 = b, so answer must be 144 and **1 = e, 4 = a.**

Using clue 1 across, possible prime numbers are 11, 13, 17 or 19. Digits are different, so answer cannot be 11. Formula states a^2+ h, ie 16+ h, so h could only be 1 or 3- but we already know that e = 1, so **h = 3** and the answer is 19. [So **d = 9**]

From clue 6 across, $2d^2=162$. From entering this in the grid, **6 = f** and **2 = c**. The answer to 2 down becomes 922, and by solving the clue to 2 down, we find that **g = 7**. The answer to 3 across is 231, and by solving the formula for this clue we find that **i = 5**. This just leaves **j** which must therefore = **8**